Breuil-Kisin Modules and Hopf Orders in Cyclic Group Rings

Alan Koch
Agnes Scott College

January 14, 2010

Abstract

For K a finite extension of $\mathbb{Q}_p$ with ring of integers R we show how Breuil-Kisin modules can be used to determine Hopf orders in K-Hopf algebras of p-power dimension. We find all cyclic Breuil-Kisin modules, and use them to compute all of the Hopf orders in the group ring $K\Gamma$ where Γ is cyclic of order p or p^2. We also give a Laurent series interpretation of the Breuil-Kisin modules that give these Hopf orders.

Let R be a complete discrete valuation ring of mixed characteristic $(0,p)$ with quotient field K and perfect residue field k. Let $e = e\left(K/\mathbb{Q}_p\right)$ be the absolute ramification index. Then R is an extension of $W := W(k)$, the ring of Witt vectors with coefficients in k, and we may write $K = K_0[x]/(E(x))$, where K_0 =Frac(W) and $E(x)$ is an Eisenstein polynomial. For any finite group Γ the group rings $R\Gamma$ and $K\Gamma$ have the structure of Hopf algebras over R and K respectively. Clearly we have $R\Gamma \subset K\Gamma$, a relationship we can express by extension of scalars: $R\Gamma \otimes_R K \cong K\Gamma$. However, if Γ is a p-group then the R-Hopf algebra $R\Gamma$ is not uniquely determined by this isomorphism, i.e. there exist other finitely generated projective R-Hopf algebras $H \subset K$ such that $H \otimes_R K \cong K\Gamma$. Such an H must necessarily contain $R\Gamma$ [Childs(2000), 5.2], and H is called an R-Hopf order in $K\Gamma$. More generally, given a K-Hopf algebra A, an R-Hopf order is a submodule of A which is an R-Hopf algebra such that the extension of scalars from R to K produces an isomorphism with A.

The classification of Hopf orders is useful in local Galois module theory as it helps in solving the normal integral basis problem [Childs and Moss(1994)], particularly Hopf orders in group rings. If p does not divide the order of the group Γ then the answer is simple: the only R-Hopf order in $K\Gamma$ is $R\Gamma$ [Childs(2000), 20.3]. Thus we consider the cases where $|\Gamma| = p^n$ for some $n > 0$. Two examples of such groups (and the only examples for $n \leq 2$) are $\Gamma = C_{p^n}$ and $\Gamma = (C_p)^n$, where C_m is the cyclic group of order m. The former case, particularly for $n \leq 3$, has been studied by Byott, Childs, Greither, Underwood et al [Byott(1993a)] [Byott(1993b)] [Childs and Underwood(2004)] [Greither(1992)] [Underwood(1994)] [Underwood(1996)] [Underwood and Childs(2006)]. In the

latter, Childs, Greither, and Smith [Greither and Childs(1998)] [Childs and Smith III(2005)] have found some Hopf orders in certain circumstances.

Our contribution in the elementary abelian case was the introduction of Breuil modules to the problem. Using Breuil's theory of "filtered free" modules [Breuil(2000)] we get a categorical equivalence between R-Hopf algebras such that the endomorphism $[p] := (\text{mult})^p \circ (\Delta \otimes 1)^p$ is trivial, and a collection of Breuil modules, specifically free $k[u]/(u^{pe})$-modules $\mathcal{M}$ with a $k[u]/(u^{pe})$-submodule $\mathcal{M}_1 \subset u^e\mathcal{M}$ and a map $\phi_1 : \mathcal{M}_1 \to \mathcal{M}$ satisfying certain properties. In [Koch(2007)] it was shown that the Hopf algebra corresponding to a rank n Breuil module $\mathcal{M}$ was a Hopf order in $(KC_p)^n$ if and only if $\mathcal{M}_1$ contained n elements $x_1, \ldots, x_n$ which are $\mathbb{F}_p$-linearly independent and such that $\phi_1(x_i) = x_i$ for all i.

Unfortunately, Breuil modules do not easily generalize to the case where Γ is not elementary abelian. The ring $k[u]/(u^{pe})$ must be replaced with the p-adic completion of the divided power envelope of $W[u]$ with respect to the ideal $(E(u))$. Furthermore, the submodule $\mathcal{M}_1$ must contain the p-adic completion of the ideal generated by $(E(u))^i/i!$ for all $i \geq 1$, making these modules hard to classify. Another drawback to using Breuil module theory for Hopf orders is that the category of Breuil modules is not abelian, and while every Hopf order H in $K\Gamma$ comes with an injection $R\Gamma \hookrightarrow H$, the corresponding monomorphism of Breuil modules is generally not one-to-one. While in [Koch(2007)] we found a criterion for a map $\mathcal{M} \to \mathcal{M}'$ of Breuil modules of the same rank to be one-to-one, in general this appears to be a difficult problem.

In this paper, we show how one can find Hopf orders in Hopf algebras of rank p^n not necessarily killed by $[p]$ using a related theory we call Breuil-Kisin modules. Along with the theory above, Breuil [Breuil(1998)] conjectured another correspondence between a certain category of modules and finite flat commutative group schemes (and hence finite projective commutative, cocommutative Hopf algebras). The conjecture, with a slight modification, was later proved by Kisin [Kisin(2006)], and provides a simplification to the theory above. A Breuil-Kisin module is a module over $W[[u]]$ with a map ϕ satisfying certain properties. These properties depend on the Eisenstein polynomial, but in a simpler manner than for Breuil modules. An indication of the usefulness of Breuil-Kisin theory is the following fact: two Breuil-Kisin modules $\mathfrak{M}$ and $\mathfrak{M}'$ correspond to generically isomorphic K-Hopf algebras if and only if $\mathfrak{M}\left[u^{-1}\right] \cong \mathfrak{M}'\left[u^{-1}\right]$, i.e. $\mathfrak{M}$ and $\mathfrak{M}'$ become isomorphic over the ring of Laurent series $W((u))$.

We start with a review of the Breuil-Kisin theory, its connection to Breuil modules as well as to R-Hopf algebras. We explain how Hopf orders are easier to identify with Breuil-Kisin modules than with Breuil modules. Then, we look at the simplest class of Breuil-Kisin modules: the ones which are generated over $W[[u]]$ by a single element. We refer to this collection as the class of cyclic Breuil-Kisin modules. Cyclic Breuil-Kisin modules can be used to classify all Hopf orders in KC_p, but no nontrivial orders in KC_{p^n} for $n \geq 2$ can be found this way. (By "nontrivial orders" we mean orders which are not RC_{p^n}, although in general a finite K-Hopf algebra need not have any R-Hopf orders

– see [Childs(2000), 20.5].) However, in the following section we construct all Hopf orders in KC_{p^2} using extensions of cyclic Breuil-Kisin modules. Finally, we show how it is possible (although at this point perhaps not practical) to describe Hopf orders in KC_{p^n} by picking n elements in $W_n((u))$ which satisfy certain properties.

We have chosen to use Breuil-Kisin theory to find Hopf orders in KC_{p^n}, but it can be used to find Hopf orders in any abelian (commutative, cocommutative) finite projective K-Hopf algebra of p-power rank. In fact, it appears that finding orders in the dual $(KC_{p^n})^*$ may be slightly easier. Thus if K contains a primitive $(p^n)^{\text{th}}$ root of unity ζ_n then we could develop the theory by considering only $(KC_{p^n})^*$ since it is isomorphic to KC_{p^n}. However, we do not insist that $\zeta_n \in K$, in contrast to many of the works cited above.

Breuil-Kisin modules have been used predominantly to study Galois representations. We hope that the results below will encourage their use in other Hopf algebra applications. For example, in [Koch(2001)] and [Koch(2005)] we classified monogenic Hopf algebras (i.e. Hopf algebras generated by a single element) over discrete valuation rings with $e = 1$ and $e \leq p-1$ respectively. In [Koch(2010)] we classified monogenic Hopf algebras regardless of ramification, however we were limited to such Hopf algebras H where $\operatorname{Spec}(H)$ was killed by p. This latter paper used Breuil modules. Monogenic Hopf algebras are important in the study of Hopf-Galois extensions (see, e.g. [Koch(2003)]). It seems likely that Breuil-Kisin modules could be used to obtain a more general classification.

Throughout this paper, R, K, K_0, E, W, e, and p are as above. Also, let $c_0 = E(0)/p$, and let $F(u) = (E(u) - u^e)/p$. All group schemes are affine, commutative, flat, and have order a power of p; likewise all Hopf algebras are finite, projective, abelian, and of p-power rank. The author would like to thank Dajano Tossici for his suggestions on Theorem 3.1.

1 Breuil-Kisin Modules

Here we review the basic theory of Breuil-Kisin modules. More details can be found in [Kisin(2006)] and [Kisin(2010)].

Let $\mathfrak{S} = W[[u]]$ and $\mathfrak{S}_n = \mathfrak{S}/p^n\mathfrak{S} = W_n[[u]]$. Let $\phi : \mathfrak{S} \to \mathfrak{S}$ be the Frobenius-semilinear (hereafter "semilinear") map extending the Frobenius on W such that $\phi\left(u^i\right) = u^{pi}$ for all $i \geq 0$. Clearly $\phi(p^n\mathfrak{S}) \subset p^n\mathfrak{S}$, so we have induced semilinear maps on $\mathfrak{S}_n$ for all n which we also denote by ϕ. For an $\mathfrak{S}$-module $\mathfrak{M}$ we define $\mathfrak{S} \otimes_\phi \mathfrak{M}$ to be $\mathfrak{S} \otimes_{\mathfrak{S}} \mathfrak{M}$, where $\mathfrak{S}$ is viewed as an $\mathfrak{S}$-module via ϕ. Explicitly,

$$\phi(s)\, s' \otimes_\phi m = s' \otimes_\phi sm$$

for all $s, s' \in \mathfrak{S}$ and $m \in \mathfrak{M}$. In particular, $1 \otimes_\phi um = u^p \otimes_\phi m$ for $m \in \mathfrak{M}$. This $\mathfrak{S}$-module is denoted by both $\mathfrak{S} \otimes_{\phi,\mathfrak{S}} \mathfrak{M}$ and $\phi^*(\mathfrak{M})$ in [Kisin(2010)].

We define the category $'(\mathrm{Mod}/\mathfrak{S})$ to be the category of $\mathfrak{S}$-modules $\mathfrak{M}$ together with a semilinear map $\phi_{\mathfrak{M}} : \mathfrak{M} \to \mathfrak{M}$ such that $E\mathfrak{M}$ annihilates $\mathfrak{M}/(1 \otimes_{\mathfrak{S}} \phi_{\mathfrak{M}})(\mathfrak{S} \otimes_\phi \mathfrak{M})$.

Here we view $(1 \otimes_{\mathfrak{S}} \phi_{\mathfrak{M}})(\mathfrak{S} \otimes_{\phi} \mathfrak{M})$ as a submodule of $\mathfrak{M}$ via the canoncial isomorphism $\mathfrak{S} \otimes_{\mathfrak{S}} \mathfrak{M} \to \mathfrak{M}$: note that $(1 \otimes_{\mathfrak{S}} \phi_{\mathfrak{M}})$ maps $\mathfrak{S} \otimes_{\phi} \mathfrak{M}$ to $\mathfrak{S} \otimes_{\mathfrak{S}} \mathfrak{M}$. Thus we require that for all $m \in \mathfrak{M}$ there exist $\{m_i\} \subset \mathfrak{M}$ and $\{s_i\} \subset \mathfrak{S}$ such that

$$Em = \sum s_i \phi_{\mathfrak{M}}(m_i).$$

As expected, an $\mathfrak{S}$-linear map $\alpha : \mathfrak{M} \to \mathfrak{M}'$ is a morphism in this category if $\alpha \phi_{\mathfrak{M}} = \phi_{\mathfrak{M}'} \alpha$.

From here on we follow convention and write ϕ for $\phi_{\mathfrak{M}}$, $\phi_{\mathfrak{M}'}$, etc. and hope no confusion will arise. Also, the Breuil-Kisin module $(\mathfrak{M}, \phi)$ is usually denoted by $\mathfrak{M}$. Finally, any unadorned tensor will be tensored over $\mathfrak{S}$ in the usual way: we will continue to use $\otimes_{\phi}$ where appropriate.

Define the subcategory (Mod FI/$\mathfrak{S}$) to be the objects in $'$(Mod/$\mathfrak{S}$) which are isomorphic as $\mathfrak{S}$-modules to a finite sum $\bigoplus \mathfrak{S}/p^{n_i}\mathfrak{S}$ for some choice of n_i's. Also, we let (Mod/$\mathfrak{S}$) be the subcategory of $'$(Mod/$\mathfrak{S}$) consisting of modules with projective dimension 1 (as an $\mathfrak{S}$-module). Alternatively, (Mod/$\mathfrak{S}$) is the subcategory consisting of extensions in $'$(Mod/$\mathfrak{S}$) of finite free $\mathfrak{S}/p\mathfrak{S}$-modules [Kisin(2006), 2.3.2]. Note that any object in (Mod FI/$\mathfrak{S}$) is necessarily an object of (Mod/$\mathfrak{S}$). We shall refer to objects in (Mod/$\mathfrak{S}$) as Breuil-Kisin modules, with the understanding that the objects in (Mod FI/$\mathfrak{S}$) are also Breuil-Kisin modules. From [Kisin(2006), 2.3.5 and 2.3.6] we have anti-equivalences between (Mod/$\mathfrak{S}$) and the category of group schemes over R; and between (Mod FI/$\mathfrak{S}$) and group schemes over R with the property that the kernel of the map $\left[p^i\right]$ is also finite flat for all i.

The proofs of the above categorical equivalences rely on Breuil modules. We briefly describe Breuil modules – see [Breuil(2000)] for a more thorough treatment, or see the summary in [Kisin(2010)]. Let

$$S = \left\{ \sum_{i=0}^{\infty} w_i \frac{u^i}{\lfloor i/e \rfloor !} \,|\, w_i \in W,\ \lim_{i \to \infty} w_i = 0 \right\} \subset K_0 [[u]]$$

and let $\mathrm{Fil}^1 S$ be the p-adic completion of the ideal generated by $(E(u))^i / i!$. The ring S is equipped with a semilinear map ϕ given by

$$\phi\left(\frac{u^i}{\lfloor i/e \rfloor !}\right) = \frac{u^{pi}}{\lfloor i/e \rfloor !} \in pS$$

and we define ϕ_1 on S to be "ϕ/p". A Breuil module consists of a triple $(\mathcal{M}, \mathcal{M}_1, \phi_1)$ where $\mathcal{M}$ is a finite free module over S, $\mathcal{M}_1$ is an S-submodule of $\mathcal{M}$ containing $\left(\mathrm{Fil}^1 S\right)\mathcal{M}$, and ϕ_1 is a semilinear map $\mathcal{M}_1 \to \mathcal{M}$ whose image generates $\mathcal{M}$ as an S-module. The morphisms are S-module maps which commute with the respective ϕ_1's. The category of Breuil modules is denoted $'$(Mod/S). If, furthermore, the Breuil module $\mathcal{M}$ is isomorphic as an S-module to a (finite) direct sum of $S/p^{n_i}S$ for various n_i's then we say $\mathcal{M}$ is an object in the subcategory (Mod FI/S). Also, in a manner analogous to the Breuil-Kisin categories we let (Mod/S) be the full subcategory of $'$(Mod/S) which contains the objects in (Mod FI/S) killed by p and is stable by extensions.

Given a Breuil-Kisin module $\mathfrak{M}$ one can obtain a Breuil module as follows. Let $\mathcal{M} = S \otimes_\phi \mathfrak{M}$, where S is viewed as an $\mathfrak{S}$-module via the map $\mathfrak{S} \to S,\ u \mapsto u$. Then define

$$\mathcal{M}_1 = \left\{ y \in \mathcal{M} \mid (1 \otimes \phi)(y) \in \mathrm{Fil}^1 S \otimes_{\mathfrak{S}} \mathfrak{M} \right\}$$
$$\phi_1 = (\phi_1 \otimes_\phi 1)(1 \otimes \phi) : \mathcal{M}_1 \to \mathrm{Fil}^1 S \otimes \mathfrak{M} \to S \otimes_\phi \mathfrak{M}$$

Then $(\mathcal{M}, \mathcal{M}_1, \phi_1)$ is a Breuil module, and this assignment is an exact, fully faithful functor (Mod/$\mathfrak{S}$)$\to$(Mod/S) which restricts to (Mod FI/$\mathfrak{S}$)$\to$(Mod FI/S). Thus one obtains a functor Gr: (Mod/$\mathfrak{S}$)$\to$(p-Gr), where (p-Gr) denotes the category of finite flat group schemes of p-power order.

It is a consequence of [Kisin(2007), 2.4.7] that two objects $\mathfrak{M}$, $\mathfrak{M}'$ in (Mod/$\mathfrak{S}$) correspond to group schemes with isomorphic generic fibers if and only if $\mathfrak{M}\left[u^{-1}\right] \cong \mathfrak{M}'\left[u^{-1}\right]$. This observation is very important for our purposes.

We can translate the anti-equivalences with group schemes to equivalences with Hopf orders. The category (Mod/$\mathfrak{S}$) corresponds to the category of R-Hopf algebras, and (Mod FI/$\mathfrak{S}$) is equivalent to the category of Hopf algebras where $H/\left[p^i\right]H$ is flat for all i. Furthermore, if $\mathfrak{M}\left[u^{-1}\right] \cong \mathfrak{M}'\left[u^{-1}\right]$ then the Hopf algebras corresponding to $\mathfrak{M}$ and $\mathfrak{M}'$ are generically isomorphic, hence they are orders in the same K-Hopf algebra.

It should be pointed out that there is also a theory of Breuil-Kisin modules for p-divisible groups. In this case $\mathfrak{M}$ is a free $\mathfrak{S}$-module, and so we have a collection of objects we could call free "Breuil-Kisin modules". We will not use these modules here, however they are vital in the correspondence involving (Mod/$\mathfrak{S}$): the condition "projective dimension 1" means that we can realize $\mathfrak{M}$ as the cokernel of free Breuil-Kisin modules, and the resulting sequence of modules corresponds to a smooth resolution of the group scheme associated to $\mathfrak{M}$.

2 Cyclic Breuil-Kisin Modules

The simplest type of objects in (Mod FI/$\mathfrak{S}$), and hence the simplest type in (Mod/$\mathfrak{S}$), are the modules $\mathfrak{M}$ which are generated over $\mathfrak{S}$ by a single element, say e_1. Such a module will be written $\mathfrak{S}_n e_1$. We will refer to such modules as *cyclic Breuil-Kisin modules*. In this section we will find all cyclic Breuil-Kisin modules. These modules all have a simple form, particularly when $n \neq 1$.

Before we begin, we will prove a result on power series which will facilitate calculations throughout the paper. For any ring T we will denote by $v : T[[u]] \to \mathbb{Z}^+$ the function given by

$$v(f) = \min\left\{ v \mid f \in u^v T[[u]] \right\},$$

which is the usual u-adic valuation when $T = k$. We will extend this to $T((u)) \to \mathbb{Z}$ as well. For $w \in W$ we will let w^ϕ denote the Frobenius.

In the case where $n = 1$ we get the simpler:

Lemma 2.1 *Let f,$h \in k[[u]]$ be nonzero polynomials. Let f_ℓ and h_m be the coefficients of the terms in f and h respectively of lowest degree. Then there exists a $g \in k[[u]]$, $g \neq 0$ such that*

$$fg = \phi(g)\, h$$

if and only if $v(f) \geq v(h)$, $v(f) \equiv v(h) \pmod{p-1}$, and if

$$f_\ell / h_m \in \left(k^\times\right)^{p-1}.$$

Furthermore, if f and h are invertible then so is g.

Proof. Since $v(\phi(g)) = pv(g)$ the conditions on $v(f)$ and $v(h)$ are obviously necessary. If we write $f = u^{v(f)} f'$ and $h = u^{v(h)} h'$ for $f', h' \in k[[u]]^\times$ we see that this equation is equivalent to

$$u^{v(f)-v(h)} f' g = \phi(g)\, h'$$

and thus we may assume that $v(h) = 0$.

Write $f = \sum f_i u^i$, $g = \sum g_i u^i$, and $h = \sum h_i u^i$ and let $j = v(g)$. Then $v(f) = j(p-1)$. By comparing u^{pj} coefficients we get

$$f_{j(p-1)} g_j = \left(g_j^\phi\right) h_0.$$

This determines g_j since $f_{j(p-1)}$ is invertible. Now suppose $g_j, g_{j+1}, \ldots, g_{j+i}$ have been chosen. If we compare u^{pj+i+1} coefficients we get

$$f_{j(p-1)} g_{j+i+1} + \cdots + f_{j(p-1)+i+1} g_j = \left(g_j^\phi\right) h_{i+1} + G$$

where G is an expression involving $h_i, h_{i-1}, \ldots, h_0$ and $g_j, g_{j+1}, \ldots, g_{j+\varepsilon}$ where ε is the largest integer such that $p(j+\varepsilon) < j+i+1$. Thus, g_{j+i+1} is determined (and in fact is unique for a fixed g_j), and by induction $fg = \phi(g)\, h$ has a solution. That the solution is invertible follows by considering valuations. ■

We are now ready to describe the cyclic Breuil-Kisin modules.

Lemma 2.2 *For $n \geq 1$ Breuil-Kisin module structures on $\mathfrak{S}_n e_1$ correspond to factorizations of $E \bmod p^n$.*

Proof. Any semilinear map on $\mathfrak{S}_n e_1$ is of the form $\phi_f(e_1) = f e_1$ for some $f \in W_n[[u]]$. In order for $(\mathfrak{S}_n e_1, \phi_f)$ to be a Breuil-Kisin module it is necessary and sufficient that $E e_1$ be in the image of $(1 \otimes \phi_f)\left(\mathfrak{S} \otimes_{\phi_f} \mathfrak{S}_n e_1\right)$; hence if $(\mathfrak{S} e_1, \phi_f)$ is a Breuil-Kisin modules there exists an $s \in \mathfrak{S}$ such that

$$E e_1 = (1 \otimes \phi_f)(s \otimes_\phi e_1) = s \phi_f(e_1) = s f e_1$$

and so $E \equiv sf \pmod{p^n}$. ■

We start by looking at cyclic Breuil-Kisin modules where $n = 1$. These correspond to R-Hopf algebras of order p. One can immediately see the parallels with the Tate-Oort classification [Tate and Oort(1970)].

Proposition 2.3 *All Breuil-Kisin modules with* $\mathfrak{M} = \mathfrak{S}_1 e_1$ *are of the form* $(\mathfrak{S}_1 e_1, \phi_{bu^r})$ ϕ_{bu^r} *for* $0 \leq r \leq e$ *and* $b \in k^\times$. *Furthermore:*

1. $(\mathfrak{S}_1 e_1, \phi_{bu^r}) \cong (\mathfrak{S}_1 e_1, \phi_{b'u^{r'}})$ *if and only if* $r = r'$ *and* $b/b' \in (k^\times)^{p-1}$.
2. *The Hopf algebra associated to* $\left(\mathfrak{S}_1 e_1, \phi_{c_0^{-1}u^e}\right)$ *is* RC_p *and the Hopf algebra associated to* $(\mathfrak{S}_1 e_1, \phi_1)$ *is* $(RC_p)^*$.
3. *The Hopf algebra associated to* $(\mathfrak{S}_1 e_1, \phi_{bu^r})$ *is an order in* KC_p *if and only if* $bc_0 \in (k^\times)^{p-1}$ *and* $r \equiv e \pmod{p-1}$.

Proof. Let $(\mathfrak{S}_1 e_1, \phi_f)$ be a Breuil-Kisin module. Write $f = u^r h$, where $h \in k[[u]]^\times$. As f is a factor of E it is clear that $r \leq e$. Let $g \in k[[u]]^\times$ be a solution to $hg = b\phi(g)$ where $b = h(0)$ – by Lemma 2.1 such a g exists. The map $\alpha : (\mathfrak{S}_1 e_1, \phi_{u^r h}) \to (\mathfrak{S}_1, e_1, \phi_{bu^r})$ given by $\alpha(e_1) = g e_1$ satisfies

$$\begin{aligned}\alpha(\phi_{u^r h}(e_1)) &= \alpha(u^r h e_1) = u^r g h e_1 = u^r b \phi(g) e_1 \\ &= \phi(g)\phi_{bu^r}(e_1) = \phi_{bu^r}(g e_1) = \phi_{bu^r}(\alpha(e_1))\end{aligned}$$

and as $g \in k[[u]]^\times$ we have an isomorphism. Now suppose $\beta : (\mathfrak{S}_1 e_1, \phi_{bu^r}) \cong (\mathfrak{S}_1 e_1, \phi_{b'u^{r'}})$ is an isomorphism, say $\beta(e_1) = g e_1,\ g \in k[[u]]^\times$ (different from the g above). Then

$$\begin{aligned}\beta\phi_{bu^r}(e_1) &= \beta(bu^r e_1) = bu^r g e_1 \\ \phi_{b'u^{r'}}\beta(e_1) &= \phi_{b'u^{r'}}(ge) = \phi(g) b' u^{r'} e_1.\end{aligned}$$

Since β commutes with the respective ϕ's we have $bu^r g = \phi(g) b' u^{r'}$. As we must have equal valuations, and since $v(g) = v(\phi(g)) = 1$, we have $r = r'$. Thus this equation reduces to $bg = \phi(g) b'$, which has a solution if and only if $b/b' \in (k^\times)^{p-1}$. This proves **1**.

To prove **2** we will find the corresponding Breuil module for $(\mathfrak{S}_1 e_1, \phi_{bu^r})$. Recall that $\mathcal{M} = S \otimes_\phi \mathfrak{S}_1 e_1$. As $pe_1 = 0$ and $\phi(p) = p$ we have $p \otimes_\phi e_1 = 0$ so we may replace S with $S_1 := S/pS$, which we will identify with $k[u]/(u^{pe})$, via the isomorphism in [Breuil(2000), 2.1.2.1], where this ring is denoted $\tilde{S}_1$. Note that under this isomorphism $\phi_1(u^e) = \phi_1(E) = c_0^p \in S_1$. Thus $\mathcal{M} = \{s \otimes_\phi e_1 \mid s \in S_1\}$ and we have

$$\mathcal{M}_1 = \{s \otimes_\phi e_1 \mid (1 \otimes \phi)(s \otimes_\phi e_1) \in u^e S_1 \otimes \mathfrak{S} e_1\}.$$

As $(1 \otimes \phi)(s \otimes_\phi e_1) = s u^r e_1$ we see that $(1 \otimes \phi)(s \otimes_\phi e_1) \in u^e S_1 \otimes \mathfrak{S} e_1$ if and only if $s \in u^{e-r} S_1$, hence

$$\mathcal{M} = u^{e-r} S_1 \otimes_\phi \mathfrak{S} e_1.$$

Finally, we compute ϕ_1:

$$\begin{aligned}\phi_1\left(u^{e-r} \otimes_\phi e_1\right) &= (\phi_1 \otimes_\phi 1)(1 \otimes \phi)\left(u^{e-r} \otimes_\phi e_1\right) \\ &= (\phi_1 \otimes_\phi 1)\left(u^{e-r} \otimes b u^r e_1\right) \\ &= (\phi_1 \otimes_\phi 1)(b u^e \otimes e_1) \\ &= b^p c_0^p \otimes_\phi e_1.\end{aligned}$$

This is the Breuil module denoted $\mathcal{M}\left(e-r,(bc_0)^p\right)$ in [Breuil, Conrad, Diamond, and Taylor(2001)]. If $b=c_0^{-1}$ and $r=e$ we get $\mathcal{M}\left(0,1\right)$, whose corresponding Hopf algebra is RC_p; if $b=1$ and $r=0$ we get $\mathcal{M}\left(e,c_0^{-p}\right)$ which gives $\left(RC_p\right)^*$ [Breuil, Conrad, Diamond, and Taylor(2001), 5.2.1].

Finally, if $(\mathfrak{M}=\mathfrak{S}_1e_1,\phi_{bu^r})$ corresponds to a Hopf order in KC_p then $\mathfrak{M}\left[u^{-1}\right]$ is isomorphic to $\left(\mathfrak{S}_1e_1\left[u^{-1}\right],\phi_{c_0^{-1}u^e}\right)$. Suppose $\gamma:\mathfrak{M}\left[u^{-1}\right]\rightarrow\left(\mathfrak{S}_1e_1\left[u^{-1}\right],\phi_{c_0^{-1}u^e}\right)$ is such an isomorphism. Then, as $\mathfrak{S}_1$-modules, each is isomorphic to the ring of Laurent series $k\left((u)\right)$. We have $\gamma\left(e_1\right)=ge_1$ for some $g_1\in k\left((u)\right)^{\times}$ and $\gamma\left(\phi_{bu^r}\left(e_1\right)\right)=\phi_{c_0^{-1}u^e}\left(\gamma\left(e_1\right)\right)$. Thus,

$$bu^rge_1=\phi\left(g\right)c_0^{-1}u^ee_1,$$

and since $v\left(\phi\left(g\right)\right)=pv\left(g\right)$ we have

$$r+v\left(g\right)=pv\left(g\right)+e$$

which implies $r-e=\left(p-1\right)v\left(g\right)$ so $(p-1)$ divides $e-r$. Writing $g=u^vg',\ g'\in k\left[[u]\right]^{\times}$ gives

$$bu^{r+v}g'=u^{e+pv}\phi\left(g'\right)c_0^{-1}$$

and since $r+v=e+pv$ (note that $v<0$) we get

$$bg'=\phi\left(g'\right)c_0^{-1},$$

which has a solution if and only if $bc_0\in\left(k^{\times}\right)^{p-1}$. ■

Remark 2.4 *More generally, one can show that* $(\mathfrak{S}_1e_1,\phi_{bu^r})$ *and* $(\mathfrak{S}_1e_1,\phi_{b'u^{r'}})$ *correspond to generically isomorphic Hopf algebras if and only if* $r\equiv r'\pmod{p-1}$ *and* $b/b'\in k^{\times}$. *Also, the first Hopf algebra is contained in the second if and only if* $r\geq r'$.

Of course, if $(\mathfrak{S}_1e_1,\phi_{bu^r})$ corresponds to a Hopf order in KC_p we may replace b with c_0^{-1} since they give isomorphic Breuil-Kisin modules. Thus:

Corollary 2.5 *The Hopf orders in* KC_p *correspond to Breuil-Kisin modules of the form* $\left(\mathfrak{S}_1e_1,\phi_{c_0^{-1}u^r}\right)$ *where* $r\equiv e\pmod{p-1}$. *If we let* $j=\left(e-r\right)/\left(p-1\right)$, *one can realize this Hopf algebra as the Larson order*

$$R\left[\frac{\sigma-1}{\pi^j}\right]\subset K\left\langle\sigma\right\rangle$$

where σ *is a generator of* C_p. *(See [Larson(1976)] for a description of Larson orders.)*

We now turn our attention to the case where $n\geq2$. We will see that the cyclic Breuil-Kisin modules fail to give many Hopf orders.

Proposition 2.6 *Suppose $n \geq 2$. Then the semilinear maps on $\mathfrak{S}_n e_1$ which give a Breuil-Kisin module structure are of the form ϕ_b or ϕ_{bE}, where b is an invertible element in W_n. Furthermore:*

1. *$Gr((\mathfrak{S}_n e_1, \phi_b))$ is of multiplicative type and $Gr((\mathfrak{S}_n e_1, \phi_{bE}))$ is étale.*
2. *We have $(\mathfrak{S}_n e_1, \phi_b) \cong (\mathfrak{S}_n e_1, \phi_{b'})$ (resp. $(\mathfrak{S}_n e_1, \phi_{bE}) \cong (\mathfrak{S}_n e_1, \phi_{b'E})$) if and only if $b/b' \in (W_n^{\times})^{p-1}$.*

Proof. As E is irreducible mod p^n, if we write $E = fs$ then either $v(f) = 0$ or e. In the first case, the map $e_1 \mapsto ge_1$, where $g \in W_n[[u]]$ is chosen so that $fg = \phi(g) b$, where $b = f(0) \in W_n^{\times}$, establishes an isomorphism $(\mathfrak{S}_n e_1, \phi_f) \to (\mathfrak{S}_n e_1, \phi_b)$. This can be shown by setting the constant term of g equal to 1 and proceeding inductively as in the proof of Lemma 2.1. If $v(f) = e$ then $v(s) = 0$ and we have $f = s^{-1}E$. In this case choose $g \in W_n[[u]]$ such that $gs^{-1} = b\phi(g)$ where $b = s^{-1}(0) \in W_n^{\times}$. This gives an isomorphism $(\mathfrak{S}_n e_1, \phi_f) \to (\mathfrak{S}_n e_1, \phi_{bE})$.

Statement **1** follows from [Kisin(2010), 1.1.15]. For **2**, let $\alpha : (\mathfrak{S}_n e_1, \phi_b) \to (\mathfrak{S}_n e_1, \phi_{b'})$ be the isomorphism given by $e_1 \mapsto he_1$. Then $bhe_1 = \phi(h) b' e_1$, and as b, b' are invertible equality holds if and only if $b/b' = h_0^{\phi}/h_0$ where h_0 is the constant term of h. A similar argument holds for the modules corresponding to the étale groups. ■

Corollary 2.7 *$Gr\left(\mathfrak{S}_n e_1, \phi_{c_0^{-1}E}\right) \cong \mu_{p^n}$ and $Gr(\mathfrak{S}_n e_1, \phi_1) \cong \mathbb{Z}/p^n\mathbb{Z}$, and hence these Breuil modules correspond to RC_{p^n} and $(RC_{p^n})^*$ respectively.*

Example 2.8 *Suppose $K = \mathbb{Q}_p[\zeta]$ where ζ is a primitive $\left(\zeta^{p^n}\right)^{th}$ root of unity. Then*

$$E = \frac{(u+1)^{p^n} - 1}{(u+1)^{p^{n-1}} - 1} = \frac{t^p - 1}{t - 1},\ t = (u+1)^{p^{n-1}}$$

is its Eisenstein polynomial [Birch(1967), Lemma 3]. In particular, $c_0 = 1$. We have a map $\alpha : \left(\mathfrak{S}_n e_1\left[u^{-1}\right], \phi_1\right) \to \left(\mathfrak{S}_n e_1\left[u^{-1}\right], \phi_E\right)$ given by $\alpha(e_1) = (1-t)^{-1} e_1$. Notice that $\phi\left((1-t)^{-1}\right) = (1-t^p)^{-1}$. Since

$$\begin{aligned}
\phi_E \alpha(e_1) &= \phi_E\left(\frac{1}{1-t} e_1\right) \\
&= \left(\frac{t^p - 1}{t - 1}\right) \frac{1}{1 - t^p} e_1 \\
&= \frac{1}{1-t} e_1 = \alpha\phi(e_1)
\end{aligned}$$

we see that α is an isomorphism. This demonstrates the well-known fact that $\mu_{p^n} \cong \mathbb{Z}/p^n\mathbb{Z}$ over a field K containing the $(p^n)^{th}$ roots of unity.

The final result of the section shows the paucity of Hopf orders in group rings arising from cyclic modules.

Corollary 2.9 *The Hopf algebra associated to* $(\mathfrak{S}_n e_1, \phi_{bE})$ *is a Hopf order in* KC_{p^n} *if and only if it is* RC_{p^n}.

Proof. Clear since every isomorphism $\left(\mathfrak{S}_n e_1\left[u^{-1}\right], \phi_{bE}\right) \to \left(\mathfrak{S}_n e_1\left[u^{-1}\right], \phi_{c_0^{-1}E}\right)$ of the form $e_1 \mapsto he_1$ has $v(h) = 0$ and hence restricts to an isomorphism $(\mathfrak{S}_n e_1, \phi_{bE}) \to \left(\mathfrak{S}_n e_1, \phi_{c_0^{-1}E}\right)$. ■

Remark 2.10 *Of course, a similar statement holds for orders in* $(KC_{p^n})^*$ *or any other* K*-Hopf algebra of dimension* p^n, $n > 2$ *which is realizable as* $H \otimes_R K$ *for some* R*-Hopf algebra* H *corresponding to a cyclic Breuil-Kisin module.*

3 Hopf Orders in KC_{p^2}

We now find the Breuil-Kisin modules corresponding to Hopf orders in KC_{p^2}. The technique presented below is similar to the calculation in [Caruso(2010)] of group schemes generically isomorphic to ("models of") $\mathbb{Z}/p^2\mathbb{Z}$. Notice that all of the cyclic Breuil-Kisin modules are objects in (Mod FI/$\mathfrak{S}$). The non-cyclic ones constructed here will not be in this category, but as they are constructed from extensions of objects in (Mod FI/$\mathfrak{S}$) they are in (Mod/$\mathfrak{S}$).

Theorem 3.1 *Let* $0 \leq j_2 < j_1 \leq e/(p-1)$ *and pick* $f \in k((u))$ *such that*

$$v\left(u^{e+j_1}\phi(f) - u^{e+j_1-(p-1)j_2} f\right) \geq e - (p-1)(j_1 + j_2)$$
$$v\left(u^{j_1-pj_2}F + \left(u^{e+j_1}\phi(f) - u^{e+j_1-j_2(p-1)} f\right)\right) \geq 0.$$

Let $\mathfrak{M} = \mathfrak{S}_2 e_1 + \mathfrak{S}_2 e_2$ *with* $pe_2 = u^{j_1-j_2} e_1$. *Let* ϕ *be the semilinear map on* $\mathfrak{M}$ *given by*

$$\phi(e_1) = c_0^{-1} u^{e-(p-1)j_1} e_1$$
$$\phi(e_2) = u^{-(p-1)j_2} c_0^{-1} E e_2 + \left(u^{e+j_1}\phi(f) - u^{e+j_1-(p-1)j_2} f\right) c_0^{-1} e_1.$$

Then $\mathfrak{M}$ *is a Breuil-Kisin module, and the corresponding group scheme has generic fiber* μ_{p^2}. *Conversely, any such group scheme isomorphic to* μ_{p^2} *over* K *but not over* R *has a Breuil-Kisin module of the above form.*

Proof. For the most part, it is easy to check that the module above produces a Breuil-Kisin module. To show that Ee_2 is in the image of $1 \otimes \phi$ we can write

$$Ee_2 = c_0 b' u^{(p-1)j_2} \phi(e_1) + c_0 u^{(p-1)j_2} \phi(e_2)$$

where $u^{e+j_1}\phi(f) - u^{e+j_1-(p-1)j_2} f = u^{e-(p-1)j_1} b'$. The map $e_2 \mapsto u^{-j_2} + pf$ (and hence $e_1 \mapsto pu^{-j_1}$) establishes the isomorphism $\mathfrak{M}\left[u^{-1}\right] \to W_2((u))$ that we need. The remainder of the proof will establish that the conditions above are necessary.

Let $\mathfrak{M}$ be a Breuil-Kisin module over $W_2[[u]]$ with $\mathfrak{M}\left[u^{-1}\right] \cong W_2((u))$, where ϕ_0 on $W_2((u))$ is the semilinear map given by $\phi_0(1) = c_0^{-1}E$. (We use the notation ϕ_0 to eliminate confusion since $\phi_0(f) = \phi(f)c_0^{-1}E$ for all $f \in W_2((u))$.) Let $\mathfrak{M}_1 = \ker\{p : \mathfrak{M} \to \mathfrak{M}\}$ and let $\mathfrak{M}_2 = \mathfrak{M}/\mathfrak{M}_1$. Then $p\mathfrak{M}_1 = 0 = p\mathfrak{M}_2$. Since $\phi(pm) = p\phi(m)$, $m \in \mathfrak{M}$ we have that $\mathfrak{M}_1$ and $\mathfrak{M}_2$ are each Breuil-Kisin modules (via $\phi|_{\mathfrak{M}_1}$ and $\bar{\phi}$ respectively). The isomorphism $\mathfrak{M}\left[u^{-1}\right] \cong W_2((u))$ carries $p\mathfrak{M}\left[u^{-1}\right]$ to $pW_2((u))$, hence $\mathfrak{M}_1\left[u^{-1}\right]$ and $\mathfrak{M}_2\left[u^{-1}\right]$ are each isomorphic to $k((u))$. Thus there exist $e_1 \in \mathfrak{M}_1$ and $\bar{e}_2 \in \mathfrak{M}_2$ such that

$$\mathfrak{M}_1 = \mathfrak{S}_1 e_1, \phi(e_1) = c_0^{-1}u^{e-(p-1)j_1}e_1,\ 0 \le j_1 \le \frac{e}{p-1}$$
$$\mathfrak{M}_2 = \mathfrak{S}_1 \bar{e}_2, \phi(\bar{e}_2) = c_0^{-1}u^{e-(p-1)j_2}\bar{e}_2,\ 0 \le j_2 \le \frac{e}{p-1}.$$

Pick $e_2 \in \mathfrak{M}$ a lift of $\bar{e}_2$. Then $\{e_1, e_2\}$ generate $\mathfrak{M}\left[u^{-1}\right]$ as a $W_2((u))$-module. Since $pe_2 \in \mathfrak{M}_1$ it follows that

$$pe_2 = u^{\varepsilon} f e_1$$

for some $f \in k[[u]]^{\times}$ and $\varepsilon \ge 0$. In fact, if $\varepsilon = 0$ then $\mathfrak{M}$ is a cyclic Breuil-Kisin module, and hence the corresponding group scheme is isomorphic to μ_{p^2}, thus we assume $\varepsilon > 0$. Applying ϕ to both sides gives us

$$p\phi(e_2) = u^{p\varepsilon}\phi(f)\phi(e_1)$$

and since $\phi(e_2) = c_0^{-1}u^{e-(p-1)j_2}e_2 + pm$ for some $m \in \mathfrak{M}$ we get

$$\begin{aligned} pc_0^{-1}u^{e-(p-1)j_2}e_2 &= u^{p\varepsilon}\phi(f)c_0^{-1}u^{e-(p-1)j_1}e_1 \\ &= u^{\varepsilon(p-1)}\phi(f)c_0^{-1}u^{e-(p-1)j_1}f^{-1}(u^{\varepsilon}fe_1) \\ &= u^{\varepsilon(p-1)}\phi(f)c_0^{-1}u^{e-(p-1)j_1}f^{-1}pe_2 \end{aligned}$$

and by comparing valuations we get

$$e - (p-1)j_2 = \varepsilon(p-1) + e - (p-1)j_1,$$

i.e. $\varepsilon = j_1 - j_2$. Furthermore we see that $\phi(f) = f$, so $f \in \mathbb{F}_p[[u^p]]^{\times}$. By replacing e_1 with $f^{-1}e_1$ we may assume $f = 1$. Thus

$$pe_2 = u^{j_1 - j_2}e_1,$$

and $j_1 > j_2$.

To determine $\phi(e_2)$ we use the isomorphism $\alpha : \mathfrak{M}\left[u^{-1}\right] \to W_2((u))$ which commutes with the ϕ's. Let $\alpha(e_2) = u^i g,\ g \in W_2[[u]]^{\times}$. By replacing e_2 by ζe_2, for some $(p-1)^{\text{st}}$ root of unity ζ we may assume $g(0) \equiv 1 \pmod{p}$. Then

$$\alpha(\phi(e_2)) = \phi_0(\alpha(e_2)) = u^{pi}\phi(g)c_0^{-1}E$$

Since $\phi(e_2) \equiv c_0^{-1} u^{e-(p-1)j_2} e_2 \pmod{p}$ we have

$$\begin{aligned}\alpha\left(c_0^{-1} u^{e-(p-1)j_2} e_2 + pm'\right) &= c_0^{-1} u^{e-(p-1)j_2} \alpha(e_2) + p\alpha(m') \\ &= u^{pi} \phi(g) c_0^{-1} E,\end{aligned}$$

for some $m' \in \mathfrak{M}$, and so

$$\alpha(e_2) \equiv u^{pi+(p-1)j_2-e} \phi(g) E \pmod{p}.$$

Since $\phi(g) E \equiv u^e \pmod{p}$ we get

$$u^i \equiv u^{pi+(p-1)j_2} \pmod{p}$$

and hence $i = pi + (p-1) j_2$, i.e. $i = -j_2$. Therefore,

$$\alpha(e_2) = u^{-j_2} + pf,\ f \in k((u)).$$

Since $\left(u^{j_2} - u^{2j_2} pf\right)\left(u^{-j_2} + pf\right) = 1 \in W_2((u))$ we get

$$\begin{aligned}\alpha(\phi(e_2)) &= \phi_0\left(u^{-j_2} + pf\right) \\ &= \left(u^{-pj_2} + p\phi(f)\right) c_0^{-1} E \\ &= \left(u^{-pj_2} + p\phi(f)\right) c_0^{-1} E \left(u^{j_2} - u^{2j_2} pf\right)\left(u^{-j_2} + pf\right) \\ &= \left(u^{-pj_2} + p\phi(f)\right)\left(u^{j_2} - u^{2j_2} pf\right) c_0^{-1} E \alpha(e_2) \\ &= \alpha\left(\left(u^{-pj_2} + p\phi(f)\right)\left(u^{j_2} - u^{2j_2} pf\right) c_0^{-1} E e_2\right).\end{aligned}$$

As α is an isomorphism we get

$$\begin{aligned}\phi(e_2) &= \left(u^{-pj_2} + p\phi(f)\right)\left(u^{j_2} - u^{2j_2} pf\right) c_0^{-1} E e_2 \\ &= \left(u^{-j_2(p-1)} + p u^{j_2} \phi(f) - u^{-j_2(p-2)} pf\right) c_0^{-1} E e_2 \\ &= u^{-j_2(p-1)} c_0^{-1} E e_2 + \left(u^{j_2} \phi(f) - u^{-j_2(p-2)} f\right) c_0^{-1} E(pe_2) \\ &= u^{-j_2(p-1)} c_0^{-1} E e_2 + \left(u^{e+j_1} \phi(f) - u^{e+j_1-j_2(p-1)} f\right) c_0^{-1} e_1.\end{aligned}$$

Now it is necessary that the right-hand side be in $\mathfrak{M}$ (as opposed to $\mathfrak{M}\left[u^{-1}\right]$), therefore there are restrictions on the choice of f. We will return to this issue at the end of the proof.

Since $\mathfrak{M}$ to be a Breuil-Kisin module, we require that that Ee_1 and Ee_2 are in the image of $1 \otimes \phi$. As $Ee_1 = c_0 u^{(p-1)j_1} \phi(e_1)$ it suffices to find $x, y \in W_2[[u]]$ such that $Ee_2 = x\phi(e_1) + y\phi(e_2)$. Thus

$$\begin{aligned}pEe_2 &= y u^{-(p-1)j_2} c_0^{-1} E p e_2 \\ pu^e e_2 &= y u^{e-(p-1)j_2} c_0^{-1} p e_2\end{aligned}$$

and hence $y = c_0 u^{(p-1)j_2} + py'$ for some $y' \in k[[u]]$. Substituting, we get

$$\begin{aligned} Ee_2 &= c_0^{-1} x u^{e-(p-1)j_1} e_1 + \left(c_0 u^{(p-1)j_2} + py' \right) \phi(e_2) \\ &= c_0^{-1} x u^{e-(p-1)j_1} e_1 + Ee_2 + c_0^{-1} py' u^{e-(p-1)j_2} e_2 + u^{(p-1)j_2} \left(u^{e+j_1} \phi(f) - u^{e+j_1-(p-1)j_2} f \right) e_1 \end{aligned}$$

and so

$$\begin{aligned} &c_0^{-1} x u^{e-(p-1)j_1} e_1 + c_0^{-1} py' u^{e-(p-1)j_2} e_2 + u^{(p-1)j_2} \left(u^{e+j_1} \phi(f) - u^{e+j_1-(p-1)j_2} f \right) e_1 = 0 \\ &\left(c_0^{-1} x u^{e-(p-1)j_1} + c_0^{-1} y' u^{e-pj_2+j_1} + u^{(p-1)j_2} \left(u^{e+j_1} \phi(f) - u^{e+j_1-(p-1)j_2} f \right) \right) e_1 = 0 \end{aligned}$$

As $e - pj_2 + j_1 > e - (p-1) j_1$, for this to have a solution we require $(p-1) j_2 + v\left(u^{e+j_1}\phi(f) - u^{e+j_1-(p-1)j_2} f\right) = v(x) + v\left(u^{e-(p-1)j_1}\right)$, i.e. $v\left(u^{e+j_1}\phi(f) - u^{e+j_1-(p-1)j_2} f\right) \geq e - (p-1)(j_1+j_2)$. If we write $u^{e+j_1}\phi(f) - u^{e+j_1-(p-1)j_2} f = u^{e-(p-1)(j_1+j_2)} b$ then we can solve the above by setting $x = c_0 b$ and $y' = 0$.

We require $\phi(e_2) \in \mathfrak{M}$, which of course is equivalent to having $c_0 \phi(e_2) \in \mathfrak{M}$. We have

$$\begin{aligned} c_0 \phi(e_2) &= u^{-j_2(p-1)} E e_2 + \left(u^{e+j_1} \phi(f) - u^{e+j_1-j_2(p-1)} f \right) e_1 \\ &= u^{-j_2(p-1)} \left(u^e + pF \right) e_2 + \left(u^{e+j_1} \phi(f) - u^{e+j_1-j_2(p-1)} f \right) e_1 \\ &= u^{e-j_2(p-1)} e_2 + \left(u^{-j_2(p-1)} u^{j_1-j_2} F + \left(u^{e+j_1} \phi(f) - u^{e+j_1-j_2(p-1)} f \right) \right) e_1 \\ &= u^{e-j_2(p-1)} e_2 + \left(u^{j_1-pj_2} F + \left(u^{e+j_1} \phi(f) - u^{e+j_1-j_2(p-1)} f \right) \right) e_1 \end{aligned}$$

and since $u^{e-j_2(p-1)} e_2 \in \mathfrak{M}$ this means we need

$$v\left(u^{j_1-pj_2} F + \left(u^{e+j_1} \phi(f) - u^{e+j_1-j_2(p-1)} f \right) \right) \geq 0$$

as desired. ■

Remark 3.2 *The second valuation condition is a bit more difficult to work with because it depends on the Eisenstein polynomial. However, suppose we pick $j_1 < j_2$ such that $e - (p-1)(j_1+j_2) \geq 0$. Then for $f \in k((u))$ so that $v\left(u^{e+j_1}\phi(f) - u^{e+j_1-(p-1)j_2} f\right) \geq e - (p-1)(j_1+j_2)$ we see that $\left(u^{e+j_1}\phi(f) - u^{e+j_1-(p-1)j_2} f\right) e_1 \in \mathfrak{M}$ and hence $\left(u^{j_1-pj_2} F + \left(u^{e+j_1}\phi(f) - u^{e+j_1-j_2(p-1)} f\right)\right) e_1 \in \mathfrak{M}$ precisely when $u^{j_1-pj_2} e_1 \in \mathfrak{M}$. Thus if $e - (p-1)(j_1+j_2) \geq 0$ then the second condition is satisfied if and only if $j_1 \geq pj_2$.*

4 Laurent Series and Hopf Orders

Since each Breuil-Kisin module $\mathfrak{M}$ which is an order in KC_{p^n} must satisfy $\mathfrak{M}\left[u^{-1}\right] \cong \left(\mathfrak{S} n e_1 \left[u^{-1}\right], \phi_{c_0^{-1}E} \right)$, as $\mathfrak{S}$-modules we have $\mathfrak{M}\left[u^{-1}\right] \cong W_n((u))$. Thus Hopf orders can be identified by looking at certain Laurent series.

As an example, let us return to the case $n = 1$. We have found that the Hopf orders correspond to Breuil-Kisin modules of the form $\left(\mathfrak{S}_1 e_1, \phi_{c_0^{-1}u^r}\right)$ with $e - r = j(p-1)$ for some j. By following the induced isomorphism $\mathfrak{M}\left[u^{-1}\right] \to k((u))$, which here can be chosen to be $e_1 \mapsto u^{-j}e_1$, we have e_1 corresponding to the Laurent series u^{-j}. Thus, u^{-j} encodes all of the information concerning this Hopf order. In other words, the set

$$\left\{u^{-j} \mid 0 \leq j \leq \left\lfloor \frac{e}{p-1} \right\rfloor \right\} \subset k((u)).$$

parameterizes all Hopf orders in KC_p.

Similarly, the Breuil-Kisin module $\mathfrak{M}$ for a Hopf order in KC_{p^2} is generated by at most two elements e_1 and e_2 such that there is an isomorphism $\alpha : \mathfrak{M}\left[u^{-1}\right] \to W_2((u))$. From the work above we see that $\alpha(e_2) = u^{-j_2} + pf$ and $\alpha(e_1) = \alpha\left(u^{j_2-j_1}pe_2\right) = pu^{-j_1}$, where $v\left(u^{e+j_1}\phi(f) - u^{e+j_1-(p-1)j_2}f\right) \geq e-(p-1)(j_1+j_2)$ and $v\left(u^{j_1-pj_2}F + \left(u^{e+j_1}\phi(f) - u^{e+j_1-j_2(p-1)}f\right)\right) \geq 0$. Thus the set

$$\begin{gathered}\left\{\left(pu^{-j_1}, u^{-j_2}+pf\right) \mid j_1 \geq pj_2,\ v\left(u^{e+j_1}\phi(f) - u^{e+j_1-(p-1)j_2}f\right) \geq e-(p-1)(j_1+j_2),\right. \\ \left. v\left(u^{j_1-pj_2}F + \left(u^{e+j_1}\phi(f) - u^{e+j_1-j_2(p-1)}f\right)\right)\right\} \subset \left(k((u))\right)^2\end{gathered}$$

parameterizes all Hopf orders in KC_{p^2}. It seems possible that one could find Hopf orders in KC_{p^n} by picking n-tuples of Laurent series satisfying certain properties.

To what extent can this idea be applied to $n > 2$? Pick $f_1, f_2, \ldots, f_n \in W_n((u))$ such that $f_1 \notin pW_n((u))$ and

$$f_i = \sum_{i=1}^{n} s_{ij}c_0^{-1}\phi(f_j),\ s_{ij} \in W_n[[u]].$$

Let $\mathfrak{M}$ be the $\mathfrak{S}$-module generated by $\{e_1, e_2, \ldots, e_n\}$ such that $\alpha : W_n((u)) \to \mathfrak{M}\left[u^{-1}\right]$, $\alpha(f_i) = e_i$ is an $\mathfrak{S}$-module isomorphism. Define $\phi : \mathfrak{M} \to \mathfrak{M}$ by $\phi(e_i) = E\alpha\left(c_0^{-1}\phi(f_i)\right)$. Since

$$\begin{aligned}Ee_i = E\alpha(f_i) &= E\alpha\left(\sum_{i=1}^{n} s_{ij}c_0^{-1}\phi(f_j)\right) \\ &= \sum_{i=1}^{n} s_{ij}E\alpha\left(c_0^{-1}\phi(f_i)\right) \\ &= \sum_{i=1}^{n} s_{ij}\phi(e_j)\end{aligned}$$

we see that $(\mathfrak{M}, \phi)$ is a Breuil-Kisin module. Furthermore, if we let ϕ_0 be the semilinear map on $W_n((u))$ given by $\phi_0(1) = c_0^{-1}E$ we get

$$\begin{aligned}\phi(\alpha(f_i)) = \phi(e_i) &= E\alpha\left(c_0^{-1}\phi(f_i)\right) \\ \alpha(\phi_0(f_i)) = \alpha\left(c_0^{-1}E\phi(f_i)\right) &= E\alpha\left(c_0^{-1}\phi(f_i)\right),\end{aligned}$$

and so $\alpha\phi_0 = \phi\alpha$ and we get:

Proposition 4.1 *There is a correspondence*

$$\{\mathbf{f} \in (W_n((u)))^n \mid \mathbf{f} = A\mathbf{\Phi}(\mathbf{f}),\ A \in M_n(W_n[[u]]),\ f_1 \not\equiv 0 \pmod{p}\},$$

where $\mathbf{f} = (f_1, f_2, \ldots, f_n)$ *and* $\mathbf{\Phi}(\mathbf{f}) = (\phi(f_1), \phi(f_2), \ldots, \phi(f_n))$; *and R-Hopf orders in* KC_{p^n}.

Proof. The only remaining detail is to show that the $\mathfrak{M}$ as constructed above is an object in (Mod/$\mathfrak{S}$) (as opposed to simply an object in $'$(Mod/$\mathfrak{S}$)). This, however, follows from the fact that there is a canonical surjection $\mathfrak{S}^n \to \mathfrak{M}$. ■

While it would be convenient to have a theory of Hopf orders based solely on the ring of Laurent series, there seem to be two obstacles to using this proposition in practice. One, it seems difficult in general to find the f_i's that satisfy the above conditions. Perhaps it would be possible to proceed inductively, in which case the matrix A would be upper-triangular. The other problem is that this is not a one-to-one correspondence: many choices of $\mathbf{f}$ lead to isomorphic Breuil-Kisin modules. For example, in the case $n = 1$ the correspondence becomes

$$\begin{aligned}\left\{f \in k((u))^\times \mid f = s\phi(f),\ v(s) \geq 0\right\} &= \left\{f = au^j + u^{j+1}f' \in k((u)) \mid a \in \left(k^\times\right)^{p-1},\ j \geq pj\right\} \\ &= \left\{f = au^j + u^{j+1}f' \in k((u)) \mid a \in \left(k^\times\right)^{p-1},\ j \leq 0\right\},\end{aligned}$$

and we see that many different choices of f correspond to the same R-Hopf order. While it is easy to determine which f are equivalent in this sense when $n = 1$, it seems much more involved for larger n.

References

[Birch(1967)] Birch, B. J. (1967), Cyclotomic fields and Kummer extensions. In: Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 85–93.

[Breuil(1998)] Breuil, C. (1998), Schmas en groupes et corps des normes. *unpublished* .

[Breuil(2000)] Breuil, C. (2000), Groupes p-divisibles, groupes finis et modules filtrés. *Ann. of Math. (2)* 152(2):489–549.

[Breuil, Conrad, Diamond, and Taylor(2001)] Breuil, C., Conrad, B., Diamond, F., Taylor, R. (2001), On the modularity of elliptic curves over **Q**: wild 3-adic exercises. *J. Amer. Math. Soc.* 14(4):843–939 (electronic).

[Byott(1993a)] Byott, N. P. (1993a), Cleft extensions of Hopf algebras. *J. Algebra* 157(2):405–429.

[Byott(1993b)] Byott, N. P. (1993b), Cleft extensions of Hopf algebras. II. *Proc. London Math. Soc. (3)* 67(2):277–304.

[Caruso(2010)] Caruso, X. (2010), Classification of integral models of $(\mathbb{Z}/p^2\mathbb{Z})_K$ via Breuil-Kisin theory. *preprint* .

[Childs(2000)] Childs, L. (2000), Taming wild extensions: Hopf algebras and local Galois module theory, volume 80 of *Mathematical Surveys and Monographs*. Providence, RI: American Mathematical Society.

[Childs and Moss(1994)] Childs, L., Moss, D. (1994), Hopf algebras and local Galois module theory. In: Advances in Hopf algebras (Chicago, IL, 1992), New York: Dekker, volume 158 of *Lecture Notes in Pure and Appl. Math.*, 1–24.

[Childs and Smith III(2005)] Childs, L., Smith III, H. (2005), Dual Hopf orders in group rings of elementary abelian p-groups. *J. Algebra* 294(2):489–518.

[Childs and Underwood(2004)] Childs, L., Underwood, R. (2004), Duals of formal group Hopf orders in cyclic groups. *Illinois J. Math.* 48(3):923–940.

[Greither(1992)] Greither, C. (1992), Extensions of finite group schemes, and Hopf Galois theory over a complete discrete valuation ring. *Math. Z.* 210(1):37–67.

[Greither and Childs(1998)] Greither, C., Childs, L. (1998), $p$elementary group schemes – constructions and Raynaud's theory. In: Hopf Algebras, Polynomial Formal Groups, and Raynaud Orders, Providence, RI: Amer. Math. Soc., volume 136 of *Mem. Amer. Math. Soc.*, 91–118.

[Kisin(2006)] Kisin, M. (2006), Crystalline representations and F-crystals. In: Algebraic geometry and number theory, Boston, MA: Birkhäuser Boston, volume 253 of *Progr. Math.*, 459–496.

[Kisin(2007)] Kisin, M. (2007), Modularity of 2-dimensional Galois representations. In: Current developments in mathematics, 2005, Int. Press, Somerville, MA, 191–230.

[Kisin(2010)] Kisin, M. (2010), Moduli of finite flat group schemes, and modularity. *Annals of Math.* To appear.

[Koch(2001)] Koch, A. (2001), Monogenic bialgebras over finite fields and rings of Witt vectors. *J. Pure Appl. Algebra* 163(2):193–207.

[Koch(2003)] Koch, A. (2003), Monogenic Hopf algebras and local Galois module theory. *J. Algebra* 264(2):408–419.

[Koch(2005)] Koch, A. (2005), Monogenic Hopf algebras over discrete valuation rings with low ramification. *J. Algebra* 286(2):405–420.

[Koch(2007)] Koch, A. (2007), Hopf orders via Breuil modules. *J. Algebra* 317(1):291–305.

[Koch(2010)] Koch, A. (2010), Monogenic Hopf algebras representing commutative p-group schemes. *preprint* .

[Larson(1976)] Larson, R. (1976), Hopf algebra orders determined by group valuations. *J. Algebra* 38(2):414–452.

[Tate and Oort(1970)] Tate, J., Oort, F. (1970), Group schemes of prime order. *Ann. Sci. École Norm. Sup. (4)* 3:1–21.

[Underwood(1994)] Underwood, R. (1994), R-Hopf algebra orders in KC_{p^2}. *J. Algebra* 169(2):418–440.

[Underwood(1996)] Underwood, R. (1996), The valuative condition and R-Hopf algebra orders in KC_{p^3}. *Amer. J. Math.* 118(4):701–743.

[Underwood and Childs(2006)] Underwood, R., Childs, L. (2006), Duality for Hopf orders. *Trans. Amer. Math. Soc.* 358(3):1117–1163 (electronic).